

REMARKS

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, claim 6 has been made dependent on claim 3. In addition, claims 19 and 19 have been cancelled, and claim 16 has been amended to include the limitations of cancelled claim 18.

The Examiner has rejected claims 1-11 and 16-19 under 35 U.S.C. 103(a) as being unpatentable over European Patent Application No. EP0752635A1 to Samar.

The Samar patent discloses a system and method to transparently integrate private key operations from a smart card with host-based encryption services, in which a computer 101 having a smart card reader 121 and an associated smart card 123 is connectable over a network 115 to a remote computer 119 or a terminal 117 each having a smart card reader 121 and optionally an associated smart card 123. If the user of the computer 101 has a smart card 123 and inserts the same into the reader 121, the computer 101 enables the transmission of messages encrypted in accordance with the contents of the smart card 123. If no smart card is inserted, the computer 101 enables the transmission of messages encrypted in accordance with the contents of a user information file 127 and encryption services 129.

The subject invention relates to the transmission and reception of encrypted signals in, for example, a cable television

system. In particular, at a headend, the cable provider encrypts a first signal in accordance with a first encryption scheme, and encrypts a second signal in accordance with a second encryption scheme. The cable provider then transmits both encrypted first and second signals. This is shown in Fig. 5, and in the specification on page 12, lines 10-13, where it is stated that the transmission station continually transmits the encrypted first and second signals, and in claim 1 which states "a receiver for receiving transmissions of the at least first signal and second signal". At a consumer's home, the receiver, which may be a set-top box, has a first embedded conditional access module for decrypting the first signal, and a second removable conditional access module (e.g., a smart card) for decrypting the second signal.

Applicants submit that Samar neither discloses or suggests that both a first encrypted signal and a second encrypted signal are transmitted at the same time. Rather, depending on communications between the computer 101 and the remote computer 119 (and/or terminal 117), a certain encryption scheme is used to encrypt messages between the computer 101 and the specific intended receiver (e.g., remote computer 119 or terminal 117).

While claim 16 discloses encrypted transmissions of at least one signal, the first conditional access module is only able to decrypt a portion of the at least one signal which may then correspond to a first signal, and the second conditional access

module is able to decrypt the whole of the at least one signal, which may then correspond to a second signal.

In view of the above, Applicants believe that the subject invention, as claimed, is not rendered obvious by the prior art, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-11, 16 and 17, claims 12-15 having been withdrawn, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by 
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611